Amendments to the Claims

1. (Previously Presented) A text messaging system for the encryption of a text message sent to a wireless terminal equipment, the text message comprising a Short Message Service (SMS) message having a User Data Header (UDH) and a text data field, the text messaging system comprising:

means for storing an equipment identification number uniquely assigned to the wireless terminal equipment, wherein the assigned equipment identification number is an International Mobile Equipment Identity (IMEI) number of the wireless terminal equipment;

means coupled to the equipment identification number storing means for encrypting the text data field content of the SMS message using only the IMEI number assigned to the wireless terminal equipment as the shared key; and

means for setting an encryption identifier in an Information Element (IE) group of the UDH of the SMS message, the encryption identifier comprising a marker in an IE data field, the IE group further comprising an Information Element Identifier (IEI) field set to indicate a presence of the marker, and an Information Element Data Length (IEDL) field set to indicate a length of the marker.

2. (Cancelled).

3. (Previously Presented) The system of claim 1 wherein the text data field of the SMS message comprises configuration commands to remotely manage the wireless terminal equipment.

4. (Cancelled).

5. (Cancelled).

6. (Previously Presented) The system of claim 1 wherein said wireless terminal equipment is a Short Message Service (SMS) receiving mobile device and said SMS message is carried over a wireless network.

7. (Cancelled).

8. (Currently Amended) The system of claim ~~7~~ 15 further comprising means coupled to the decrypting means for processing or rejecting the decrypted SMS message.

9. (Previously Presented) The system of claim 1 wherein the means for generating an encrypted SMS message further comprising means for processing an encryption algorithm to compute a bit string using said assigned IMEI number as the shared key and the text data field content.

10. (Currently Amended) The system of claim ~~7~~ 15 wherein the means for decrypting the received encrypted SMS message further comprising means for processing a decryption algorithm using said IMEI number as the shared key and the received encrypted SMS message content.

11. (Currently Amended) A method for authenticating a text message sent by a text messaging system to a wireless terminal equipment having means for storing an International Mobile Equipment Identity (IMEI) number, the text messaging system comprising means for storing an IMEI number uniquely assigned to the wireless terminal equipment, and wherein the text message comprises a Short Message Service (SMS) message having a User Data Header (UDH) and a text data field, the method comprising the steps of:

at the text messaging system:

encrypting the text data field content of the SMS message using only the IMEI number assigned to the wireless terminal equipment as the shared key;

setting an encryption identifier in an Information Element (IE) group of the UDH of the SMS message, the encryption identifier comprising a marker in an IE

data field, the IE group further comprising an Information Element Identifier (IEI) field set to indicate a presence of the marker, and an Information Element Data Length (IEDL) field set to indicate a length of the marker; and

sending the encrypted SMS message to the wireless terminal equipment;

at the wireless terminal equipment:

receiving the encrypted SMS message;

determining if the received encrypted SMS message contains an IMEI number as a shared key encryption; and

decrypting the received encrypted SMS message using the IMEI number of said wireless terminal equipment as a shared key.

12. (Previously Presented) The method of claim 11 further comprising after the receiving step, the step of determining if the encrypted SMS message contains configuration commands to remotely activate the wireless terminal equipment.

13. (Cancelled).

14. (Cancelled).

15. (New) A text messaging system for the encryption of a text message sent to a wireless terminal equipment, the text message comprising a Short Message Service (SMS) message, the text messaging system comprising:

means for storing an equipment identification number uniquely assigned to the wireless terminal equipment, wherein the assigned equipment identification number is an International Mobile Equipment Identity (IMEI) number of the wireless terminal equipment;

means coupled to the equipment identification number storing means for encrypting the text data field content of the SMS message using only the IMEI number assigned to the wireless terminal equipment as the shared key;

means for setting an encryption identifier;

means for storing an IMEI number;

means for receiving the encrypted SMS message;

means for determining if the received encrypted SMS message contains an IMEI number as a shared key encryption; and

means for decrypting the received encrypted SMS message using the stored IMEI number of said wireless terminal equipment.

16. (New) A method for authenticating a text message sent by a text messaging system to a wireless terminal equipment having means for storing an International Mobile Equipment Identity (IMEI) number, the text messaging system comprising means for storing an IMEI number uniquely assigned to the wireless terminal equipment, and wherein the text message comprises a Short Message Service (SMS) message, the method comprising:

at the text messaging system:

encrypting the text data field content of the SMS message using only the IMEI number assigned to the wireless terminal equipment as the shared key;

setting an encryption identifier in the SMS message; and

sending the encrypted SMS message to the wireless terminal equipment;

at the wireless terminal equipment:

receiving the encrypted SMS message;

determining if the received encrypted SMS message contains an IMEI number as a shared key encryption;

decrypting the received encrypted SMS message using the IMEI number of said wireless terminal equipment as a shared key; and

processing or rejecting the decrypted SMS message based on the decryption result.